UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,231	07/31/2001	Brian J. Matt	NA01-00101	6007

28875 7590 03/03/2006

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
09/921,231	07/31/2001	Brian J. Matt	NA01-0010

EXAMINER
Davis, Zachary A.

ART UNIT	PAPER
2137	20060221

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

NOTICE OF NON-COMPLIANT AMENDMENT

Response to Amendment

1. The amendment filed on 13 December 2005 is considered non-compliant because it has failed to meet the requirements of 37 CFR 1.121. In order for the amendment document to be compliant, correction of the following item is required:

The amendments to the claims have not been made according to the requirements of 37 CFR 1.121(c)(2). The text of any deleted subject matter **must** be shown by **strikethrough** except that **double brackets** may be used to show deletion of **five or fewer consecutive characters** or if strikethrough cannot be easily perceived (e.g. the numeral 4) (emphasis added). The Examiner notes that it appears that deleted subject matter in at least Claims 1, 18, and 20 (the phrase "at least in part") has been indicated only by **single brackets** before and after the deleted matter. Single brackets are not an acceptable manner of showing deleted subject matter.

The applicant is required to submit a corrected claim amendment section including directions that the corrected version of the claims be entered. **Only the corrected section** of the non-compliant amendment document must be submitted (in its entirety), i.e., the entire "Amendments to the claims" section of the applicant's amendment document must be re-submitted.

2. Since the non-compliant amendment is a reply to a NON-FINAL OFFICE ACTION, and since the amendment appears to be a bona fide attempt to be a reply (37 CFR 1.135(c)), applicant is given a TIME PERIOD of ONE MONTH (not less than 30 days) from the mailing of this letter within which to re-submit the corrected section which complies with 37 CFR 1.121 in order to avoid abandonment. EXTENSIONS OF THIS TIME PERIOD ARE AVAILABLE UNDER 37 CFR 1.136(a).

Response to Arguments

3. The Examiner will not respond to Applicant's remarks at this time with the following exceptions:

4. Regarding the rejections of Claims 1, 8, 11, 18, and 20 under 35 U.S.C. 112, second paragraph, specifically in reference to the claimed limitations of "verifying the hash value", Applicant again asserts that deletion of the language limiting the location of the hash values provides claim breadth; Applicant also asserts that Claim 8 has been "clarified" to overcome indefiniteness. Regarding the alleged clarification of Claim 8, and also the language of Claim 11, the Examiner believes that the limitations of "validating the hash value" in Claim 8 and "verifying the hash value" in Claim 11 **still render the claims indefinite** because it is **not clear** whether these limitations refer to the first verification of the hash value (see Claim 1, page 3, line 5 of the present response) or to the second verification of the hash value (see Claim 1, page 3, line 13 of the present response).

Regarding Applicant's assertion that the removal of the limiting language provides claim breadth, Applicant further argues that the Examiner cited Figure 6 to assert that the locations of the hash verifications is vital to the functioning of the claimed protocol. First, the Examiner notes that Figure 6 itself was not cited as support, but rather all of the supporting description of Figure 6 at pages 13-16 of the specification, with specific reference to paragraphs 0061 and 0063; the Examiner additionally notes that Applicant cites the very same paragraphs at page 13 of the present response. Although the Examiner concedes that the specification does not explicitly disclose the locations of the hash verifications as "vital", the Examiner nevertheless **maintains** that omission of the locations of the hash verifications **renders the claims indefinite**. The Examiner notes that the locations of other functions are claimed (e.g. sending of messages from one location to another, recreating a key at the KDC, etc.); the Examiner again asserts that it is clear from the cited portion that one of the hash verifications takes place at the second node (page 15, paragraph 0061 of the present specification) and the other takes place at the first node (page 15, paragraph 0063). Therefore, because the claim recites locations for other operations performed and the specification details where the hash verifications are to be performed, the Examiner believes that omission of the locations of the hash verifications renders the claims indefinite. Further, because there is **no distinction drawn** between the two hash verifications, it is **impossible to determine** which hash verification is being referenced in Claim 1 (at page 3, line 16 of the present response), in Claim 18 (at page 7, line 26 of the present response), or further in dependent Claims 8 and 11 (as noted above).

5. Regarding the art rejections, on page 16 of the present response, in the last paragraph, Applicant **misquotes** a cited portion of the Menezes reference (*Handbook of Applied Cryptography*). The insertion of the word "are" in the quoted phrase "[d]ata origin authentication mechanisms [are] based on shared secret keys (e.g. MACs)" (emphasis and bracketing Applicant's) **fundamentally alters** the meaning of the quoted section. In the original phrase "Data origin authentication mechanisms based on shared secret keys (e.g. MACs) do not allow" (original at Menezes, page 361, below Definition 9.77), it is clear that the parenthetical example of MACs is intended to modify the entire phrase "data origin authentication mechanisms based on shared secret keys" and not merely "shared secret keys" as asserted by Applicant. However, Applicant's manipulation of the quoted portion by insertion of "are" would alter the meaning of the quoted section so that it appears that the parenthetical example of MACs modifies only "shared secret keys". It is clear that this is not the intended meaning of the cited portion.

The Examiner therefore respectfully disagrees with Applicant's assertion that "Menezes expressly discloses that MACs are an example of a shared secret key". In addition to the plain meaning of the unaltered cited portion, the Examiner believes that Menezes provides ample additional evidence that a MAC is **based on** a secret key. See, for example, page 33, the last paragraph of section 1.9, "Hash Functions" where MACs are described as "hash functions which involve a secret key"; also see page 360, Figure 9.8(a) where a secret key is an **input** to a MAC algorithm and a MAC is output. See also Schneier, *Applied Cryptography*, portions of which were cited in the Office

action mailed 07 January 2005, noting, for example, page 31, under the heading "Message Authentication Codes", where a MAC "is a one-way hash function **with the addition of** a secret key".

6. The Examiner's response to the above arguments is not to be taken as acquiescence in whole or in part to any of Applicant's other remarks or arguments. The remainder of Applicant's remarks will be addressed when an amendment that is fully compliant under 37 CFR 1.121 has been resubmitted. Although Applicant is only required to resubmit the corrected section (i.e. the listing of Claims), Applicant is entitled to resubmit the entire amendment and/or submit further remarks addressing the arguments above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER